REGLAMENTO DE CIBERSEGURIDAD SOMBRERO BLANCO ACADEMY

ÍNDICE

I. Objetivo **3**
II. Alcance **3**
III. Principios Rectores **3**
IV. Seguridad Operacional y Técnica **4**
4.1 Gestión de Credenciales 4
4.2 Protección de Infraestructura 4
4.3 Control de Acceso y Privilegios 4
V. Gestión de Incidentes de Ciberseguridad **4**
5.1 Notificación Obligatoria 4
5.2 Clasificación de Incidentes 5
5.3 Canal de Reporte 5
VI. Normas para Estudiantes y Docentes **5**
VII. Protección de Datos y Privacidad **5**
VIII. Evaluaciones de Seguridad y Auditorías **6**
IX. Formación y Concienciación **6**
X. Sanciones y Responsabilidades **6**
XI. Disposiciones Finales 6

I. Objetivo

Establecer las directrices, normas y responsabilidades en materia de ciberseguridad que deben ser observadas por todos los usuarios, colaboradores, estudiantes, docentes, proveedores y entidades asociadas al Grupo Sombrero Blanco Ciberseguridad (en adelante, "SBC y/o SBA"), con el fin de proteger la confidencialidad, integridad y disponibilidad de los activos digitales, plataformas, infraestructuras tecnológicas y servicios asociados.

II. Alcance

Este reglamento aplica a:

- Sombrero Blanco Academy y todos sus programas académicos y plataformas.
- Equipos técnicos, administrativos y académicos.
- Entidades colaboradoras, proveedores de tecnología y consultores externos.
- Cualquier usuario que acceda a sistemas o infraestructuras de SBA.

III. Principios Rectores

- Seguridad por diseño y por defecto.
- Prevención, detección, respuesta y recuperación.
- Responsabilidad compartida.
- Cumplimiento normativo y ético.
- Concienciación y formación continua en ciberseguridad.

IV. Seguridad Operacional y Técnica

4.1 Gestión de Credenciales

- Toda cuenta de acceso a sistemas de SBA deberá estar identificada, ser personal, no transferible y con autenticación robusta.
- Se exigirá autenticación multifactor (MFA) para todo acceso privilegiado o remoto.
- Las contraseñas deberán renovarse cada 90 días y cumplir con complejidad mínima definida por la política técnica de SBA.

4.2 Protección de Infraestructura

- Toda plataforma, servidor o laboratorio deberá mantenerse actualizado y con parches de seguridad al día.
- Se exigirá cifrado de datos en reposo y en tránsito, especialmente en entornos con información sensible o de clientes.
- Se prohíbe el uso de software no autorizado o sin licencia.

4.3 Control de Acceso y Privilegios

- El acceso a información se asignará bajo el principio de mínimos privilegios y necesidad de conocer.
- Todo cambio de roles, egreso, o baja de funciones deberá implicar la revocación inmediata de accesos.

V. Gestión de Incidentes de Ciberseguridad

5.1 Notificación Obligatoria

Cualquier evento que comprometa, o potencialmente comprometa, la seguridad de los activos digitales de SBA deberá ser reportado **dentro de las primeras 2 horas** al Centro de Operaciones de Seguridad (SOC) o al correo designado para incidentes (csoc@sombrero-blanco.com).

5.2 Clasificación de Incidentes

Los incidentes se categorizarán en:

- **Críticos**: filtración de datos, ransomware, acceso no autorizado, ataques dirigidos.
- **Altos**: fallos de seguridad explotables, malware detectado en equipos clave.
  Medios/Bajos: errores de configuración, accesos fallidos repetidos, phishing sin descarga.

5.3 Canal de Reporte

- Incidentes: csoc@sombrero-blanco.com
- Fallas técnicas o vulnerabilidades: soporte@sombreroblanco.academy
- También se habilita un formulario interno en la Intranet SBC para notificaciones automatizadas (valido para colaboradores).

VI. Normas para Estudiantes y Docentes

- Queda estrictamente prohibido realizar ataques fuera de los laboratorios diseñados para pruebas, o intentar acceder a sistemas reales no autorizados.
- Toda evidencia generada en ejercicios prácticos debe resguardarse exclusivamente en los entornos autorizados.
- El uso de herramientas ofensivas está restringido al marco curricular y con acompañamiento docente.

VII. Protección de Datos y Privacidad

- Todo tratamiento de datos personales deberá ajustarse a la Ley N° 19.628 y futuras actualizaciones de protección de datos en Chile, y cumplir con estándares como la Ley 21.663 y referencias del GDPR en proyectos internacionales.
- SBA no tolerará la exposición, uso indebido o comercialización de datos generados dentro de sus plataformas.

VIII. Evaluaciones de Seguridad y Auditorías

- Todos los sistemas tecnológicos críticos estarán sujetos a evaluaciones periódicas como: pruebas de penetración, análisis de vulnerabilidades y revisiones de cumplimiento.
- Se podrá aplicar monitoreo continuo a redes, tráfico y comportamiento de usuarios en conformidad con la normativa interna de SBA.

IX. Formación y Concienciación

- Todo colaborador y estudiante deberá aprobar anualmente una capacitación en ciberseguridad básica.
- Los nuevos integrantes de SBA recibirán inducción específica sobre prácticas seguras en el uso de sistemas.
- Se promoverán campañas internas de seguridad, ejercicios de phishing simulado y actualización sobre amenazas emergentes.

X. Sanciones y Responsabilidades

El incumplimiento de este reglamento podrá dar lugar a:

- Suspensión de accesos y privilegios tecnológicos.
- Sanciones académicas o laborales.
- Acciones legales y denuncias a organismos reguladores, si corresponde.

XI. Disposiciones Finales

- El presente reglamento es complementario a las políticas de uso de laboratorios, plataformas LMS, reglamentos internos y contratos de confidencialidad.
- SBA podrá actualizar este reglamento conforme a la evolución de amenazas, tecnologías y cambios regulatorios.
- Toda persona vinculada al Grupo Sombrero Blanco declara conocer y aceptar este reglamento al momento de su incorporación a la organización.

Documento vigente a contar de 12 de enero del 2020 a la actualidad.

Sombrero Blanco Academy – Dirección Académica.

Firmado:

Diego Muñoz
Chief Executive Officer
Sombrero Blanco Ciberseguridad

Felipe García
Director Académico
Sombrero Blanco Academy

Boris González
Secretario General
Sombrero Blanco Academy

Construyamos juntos Ciberseguridad !

Conversemos

Minimizar las amenazas o los riesgos que pueda tener su negocio son fundamentales para un desarrollo economico seguro y una continuidad laboral exitosa

https://sombrero-blanco.com

contacto@sombrero-blanco.com
contacto@sombreroblanco.cl

+56 954154368
+56 951790476